

**NOVA SCOTIA FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY
REVIEW OFFICE**

***ADDRESS TO THE NOVA SCOTIA ASSOCIATION OF MUNICIPAL ADMINISTRATORS
- NOVEMBER 7, 2003 - DARCE FARDY REVIEW OFFICER***

Five years ago, in this job, I saw no evidence that the people of Nova Scotia had any interest in personal privacy issues.... or in holding public bodies, and others, accountable for protecting their personal information. That may be because they were trusting souls and expected public bodies to be careful with their personal information. Or it never occurred to them that they should at least seek assurances that their personal information would be used appropriately.

Let me tell you this is changing and, those who collect, use and disclose personal information are going to be held to account.. Nova Scotians, like other Canadians, are thinking about it more and more.... They're showing concern for the security of the personal information they are obliged to provide for government and other services. Interest in personal privacy protection is growing, as it should..

You may have noticed that Nova Scotians are raising objections to video surveillance in public areas, albeit in too small numbers. They have expressed concerns about the possible introduction of ID cards, and, of course, about the security of their health information. They have complained to me that they are being asked for their Social Insurance Numbers when they want to rent an apartment. University students have complained that the

personal information they must provide is not always used for the reasons it was collected. They are becoming aware. And more and more of them will be watching how their personal information is handled.

So let's step back and ask ourselves what privacy means. Ontario's Information and Privacy Commissioner, Ann Cavoukian co-authored a primer on personal privacy titled "WHO KNOWS? - Safeguarding your privacy in a networked world". They defined privacy as something that we enjoy every day, that we take for granted; that we would miss if we didn't have.

The definition used more than a hundred years ago by a famous American jurist, Justice Brandeis of the Supreme Court, is my favourite: Privacy is "the right to be let alone". I don't know if Justice Brandeis could see into the future and predict the perils to privacy in electronic data bases, video surveillance, ID cards etc.

Listen to the Chairman of Intel, who ought to know:

"Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset."

The authors of the WHO KNOWS? admitted privacy is easy to recognize but hard to describe. Another American jurist likened it to defining pornography: he couldn't define it but he knew it when he saw it.

To paraphrase Alberta's Information and Privacy Commissioner, one of the problems with trying to protect your privacy is that it is often lost in dribs and drabs, not in one fell swoop, unless you are sent to jail. Often times your privacy may be invaded and you don't know it.

Privacy is not an absolute right. We couldn't survive if we were not prepared to share some of our personal information. And governments and other public bodies couldn't function. But how much must we share and for what reason? And what happens to that information? More and more we want to have control of the personal information people have on us.... and we want to be free of prying eyes.

And so, in the absence of any major concern among the citizens until recently, we are fortunate that the legislature of Nova Scotia and those of all of the provinces and territories, as well as the federal government, saw the need to limit the power of public bodies to collect, use and disclose personal information. Legislators and parliamentarians, perhaps without realizing it, recognized that the powers of governments, universities, hospitals and school boards, and the police, to persuade, perhaps coerce, individuals to give up personal information about themselves, and about their lives, must be limited

to ensure there is a proper balance between the rights of the state and individual rights.

Part XX of the *Municipal Government Act* is not only about access although I'm sure that has been the preoccupation. It is also about protecting personal privacy.

Your municipalities are subject to, and have been for several years, privacy as well as access legislation in Part XX of the M.G.A.. (In less than two months, the private sector in all provinces, will be subject to similar obligations as those placed on "public bodies". *PIPEDA, the Personal Information Protection and Electronic Documents Act* comes into force on January 1, 2004. Only those provinces which pass their own "substantially similar" legislation will not be subject to the federal legislation. Nova Scotia will certainly not have such legislation by the first of the year but I hope the government will introduce its own legislation later.)

In order to provide a wide range of public services, municipalities collect and maintain personal information on thousands of Nova Scotians. They must have the personal information on those they serve. However, they hold that personal information in trust.

Like governments..., hospitals and universities gather the personal information on an amazing amount of people. In the case of hospitals it

would be a person's most intimate personal information.

Electronic government (e-government), the new buzzword, requires that special safeguards be taken to protect the personal information gathered.

These safeguards are "security" and "confidentiality". Security is the process required to protect personal information, and "confidentiality" is the duty to keep secret personal information entrusted to you.

There are two components to electronic government: placing information on line for easy accessibility by constituents; and enabling on line transactions. The second component is the tough one, presenting the most privacy challenges.

The rules laid out in 483 to 487 reflect recognized privacy principles, called Fair Information Practices. They are:

- Only personal information that is really needed should be collected. Some gatherers may think they need it or may think they should ask for it just in case. That approach does not meet proper practice.
- Where possible it should be collected directly from the individual to whom it pertains.
- The individual should be told why the information is needed.
- The information should be used only for that intended purpose.

- The information should not be used for other (secondary) purposes without the consent of the individual.
- Individuals should be given the opportunity to see their personal information and correct it if it is wrong.

Section 483 requires a municipality to make every reasonable effort to ensure the personal information gathered is accurate; make reasonable security arrangements; and keep the information for a year so that the individual the information is about can see it if she/he wants to. After that it should not be retained unless it is still being used for the purpose for which it was collected.

Section 484 obliges municipalities to accept requests from individuals to change their personal information if they feel it is incorrect.

Section 485 provides the rules for using and disclosing personal information in your files.

The federal interim Privacy Commissioner, in a recent speech to Ontario government privacy officers, made the point that although we often describe consent as the cardinal value for personal information practices, this plays a less significant role in the public sector than it does in the private sector because “public bodies collect, use and disclose a great deal of personal information on a compulsory basis”.

You will notice that Section 483 of the M.G.A. (Collection of personal information) contains no requirement for consent. Instead public bodies can collect personal information only if expressly authorized by an enactment, for law enforcement purposes or if the personal information relates directly to, and is necessary for, an operating program.

Consent may be required for the disclosure and use of personal information. Not for the collection.

When we speak of consent [s.485(1)and (2)], it should be an informed consent. To the extent possible the individual must have enough information to make an informed decision on the disposition of her or his personal information. They should understand what they are agreeing to. People in need or under stress are likely to sign anything if it will get them the services they need. A hospital administrator and I were discussing this at one time and we both recognized that many patients about to undergo surgery are in no frame of mind to provide informed consent. Nor are students, about to enroll in university... they don't want hassles. So it is the responsibility of public bodies to make every effort to explain.

Section 485(2)(f) allows a municipality to disclose personal information "to an officer or employee of a municipality if the information is necessary for the performance of the duties of, or for the protection of the health and safety of, the officer or employee." You will have to tell me how often this happens

and to whom you provide the information.

Section 485(2)(l) allows a municipality to disclose personal information to a law enforcement agency to assist in an investigation “undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result”.

Let me add a caution. You should question any officer or employee who tells you she or he needs the personal information of someone in your files. You should challenge it. You perhaps might want to ask for the request in writing. (I am not, of course, familiar with your practices so this may already be done. I hope it is.) People have trusted you with their personal information and would not expect that you would let it out of your hands without a legitimate and good reason.

We know our police, faced day in and day out with the job of trying to keep us all safe, may feel they could do their jobs better, at times, if they had more information on individuals. They might be hard to turn down. In my view, the legislators expected you to define s.485(2)(f) and (l) narrowly and the municipality must be satisfied there is a real safety issue or that there is a law enforcement proceeding or likely to proceed. Part XX of the M.G.A needs to be read and interpreted carefully

Alberta's information and privacy commissioner issued a warning for those

using e-government.

“Part of the problem with data bases is that they are never limited to one use. So, for example, a record of your dealings with your provincial government might not do much harm insofar as it is only a record of your dealings with that government. But invariably someone will find another use for this information. Law enforcement agencies, for example, are always very eager to obtain access to whatever data bases they can about individuals. It is their nature to believe that the more information they have about people the better able they will be to solve crimes. But the information resulting from your e-government relations was not intended to be used for law enforcement.

When this information gets turned to a different purpose, this is called function creep and this begins to pose serious threats to privacy.”

I think I understand the frustration of the police whom all citizens are expected to assist. So I ask you to remember your responsibilities under the Act and resist pressure to disclose personal information which you hold in trust.

In many jurisdictions public bodies are encouraged, and in some cases obliged, to adopt the practice of completing what are called Privacy Impact Assessments (PIA's).

Canada is the first country in the world to make PIA's mandatory for all federal governments and agencies. The federal Treasury Board makes PIA's a condition of funding.

The business of developing PIA's may appear daunting, but as the federal Privacy Commissioner explains in his last annual report, PIA's are simply an assessment of how and how much, a program or activity affects the privacy of individuals. The PIA process allows you to segregate privacy issues and address them in a comprehensive manner. Conducting a privacy assessment is also an effective way of engaging a team of people from technology, policy and legal, to work together to identify and resolve data protection problems. Four prominent Canadian privacy advocates address PIA's in *Annotated Guide to PIPEDA* (Published by Irwin Law Inc.). They provided a list of generic categories of information that should be considered in any privacy impact assessment. To name a few of the 26 listed: A description of the program, its goals, the need for it, its key objectives, the information collected, the source of the data, consent, and access rights of individuals to their personal data.

Some of this kind of assessment may already be done in an informal way by Nova Scotia municipalities. I recommend a more formal process and though, it may consume your time when you think you could be doing other things, in the long run it will save you time. I suggest you start the PIA system when developing any new programs that involve the need for a significant amount of personal information.

Our office is small but we are prepared to sit down with you anytime help you prepare a PIA.

While preparing PIA's and examining the security of the personal information you gather and use, you should also give thought to what you should do if there is a leak. And there probably will be. This year a reporter in Toronto called me to say she was searching the Nova Scotia Government website and came across job applications... not job postings but applications from those wanting jobs. The Public Service Commission acted quickly to plug the leak and notified the people whose applications had appeared. It is satisfied it knows how it happened.

So what should you do when it happens?

- Own up! Tell the appropriate staff immediately;
- Notify the individuals whose personal information has been leaked;
- Conduct an investigation immediately, make a report on the findings and quickly implement any recommendations;
- When that's done get back to the individuals you have notified and try to resolve their concerns.

One important ingredient to be used in protecting personal privacy is not found among the millions of words written about privacy.... and that is "common sense". Think about it. Ask yourself the questions: Would I want this personal information collected and shared if it were mine? Do we really need some of this personal information?

Some of the personal information may appear benign... like addresses and telephone numbers. To most people they might be. To a woman who has left

her abused partner, such information can be dangerous.

My intention here today is not to try to tell you how to do your jobs but encourage you to do them with the least effect on citizens' personal privacy.

In closing let me say there are weaknesses in our FOIPOP legislation with respect to the protection of privacy. It should, but doesn't, provide the Review Officer with the mandate to investigate privacy complaints or to audit the privacy protection practices of public bodies. Public bodies should be obliged to consult the Review Officer. I have asked for amendments in the provincial and municipal acts to provide that power to the Review Officer. This will come. I hope it is sooner rather than later.

And, finally, municipalities would be providing a worthwhile service to their citizens if they appointed Privacy Officers. That could be a full time job in larger municipalities and part-time in smaller ones. But you need someone whose responsibility it is to raise privacy issues for discussion and who has the authority to approve or recommend changes to policies respecting the collection and use of personal information. You should urge the powers that be that this position needs to be created. I anticipate that a privacy officer will, in time, be one of the most sought after providers of advice in the office.

Thank you!